# Attachment A

# Identity & Access Management Standard

| SUBJECT: | IDENTITY AND ACCESS MANAGEMENT TECHNOLOGY STANDARD | ADOPTION DATE: | 00/00/0000 |
|---|---|---|---|
| REQUESTER: | STANDARDS COMMITTEE | | |
| APPROVER(S): | COUNTY BOARD OF SUPERVISORS | | |
| VERSION: | 1.0 | PAGE: | PAGE 1 OF 2 |

## I. Standard Overview

Microsoft is the County standard for identity and access management (IAM) technology and provides a single source of truth for identity. Microsoft Azure AD will be the standard identity provider (IdP) for cloud applications. An on-premise Microsoft Active Directory will continue to be available as long as necessary. Microsoft's Active Directory (Azure and on-premise) has been our de facto directory services and access management provider since 2001. With the County's commitment to M365, using Microsoft as our IAM tool makes the most sense.

## II. Standard Origin

PCMG IT Security Assessment 2019 – 2020 recommendation "Implement a Countywide Identity and Access Management system"
Countywide Information Technology Strategic Plan, Goal 4

## III. Scope

This standard applies to:
- Any identity used to access the County or County resources
- Any application/system used in support of County operations

This includes, but is not limited to, computers, employees (current and former), contractors, consultants, temporaries, volunteers, interns, and other workers at the County, including all personnel affiliated with third parties.

## IV. Definitions

IAM - Identity Access Management is a security, risk management and business discipline. It encompasses practices, processes and technologies that manage the identities and entitlements of people, services and things, and the relationships between, and trust associated with, them. Effective IAM technologies equip IAM leaders and their teams to provide the right access for the right reasons. They enable the right interactions at the right time to help drive desired business outcomes and digital experience goals.

IdP - Identity Provider is a system that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network. Identity providers offer user authentication as a service.

Directory Services – A common data repository for maintaining information about users, devices, and resources. This information allows system and network administrators to control access to applications and resources. This repository is a significant piece of an organization's Identity Security strategy.

**COUNTY OF SANTA BARBARA**
**INFORMATION TECHNOLOGY STANDARD REQUEST**

| SUBJECT: | IDENTITY AND ACCESS MANAGEMENT TECHNOLOGY STANDARD | ADOPTION DATE: | 00/00/0000 |
|---|---|---|---|
| REQUESTER: | STANDARDS COMMITTEE | | |
| APPROVER(S): | COUNTY BOARD OF SUPERVISORS | | |
| VERSION: | 1.0 | PAGE: | PAGE **2** OF **2** |

V.  Standard Application

Any cloud-based systems will leverage Azure AD for authentication. On-premise applications will leverage Microsoft Active Directory unless an exception is granted by the CISO. This standard will not be applied retroactively.

VI.  Related Standards:

None

VII.  Referenced Documents:

Countywide Information Technology Strategic Plan Fiscal Years 2019-20 through 2022-23 (Countywide Technology Strategic Plan 2019-2023 (civicplus.com))